TOP ATTACKS AND BREACHES

- The Cuba ransomware gang has claimed responsibility for the cyberattack on The Philadelphia Inquirer, the largest newspaper in Philadelphia. The newspaper was hit by ransomware on May 14th, leading its IT team to shut down computer systems to prevent further damage. The attack also temporary disrupted the distribution of the print newspaper.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.Cuba.ta.*)

- The Indian manufacturing plant responsible for producing Suzuki motorcycles has been shut down due to a cyberattack, which has been impacting the business since May 10. It has been reported that the production of bikes and scooters has been temporarily suspended.

- The BlackByte ransomware gang has launched an attack against the City of Augusta, a major city in Georgia, U.S. The attackers are demanding a ransom of $400,000 to delete the stolen information. BlackByte has already leaked a 10GB sample of what they claim to be sensitive data from the victim.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.Blackbyte.ta.*)

- The North Korean APT group known as Kimsuky has launched a campaign targeting North Korea-focused information services, human rights activists, and organizations providing support to DPRK defectors. Kimsuky has made extensive use of less common TLDs during their malicious domain registration process, like abusing .space, .asia, .click, and .online TLD's.

  Check Point Anti-Bot Blade provides protection against this threat (Backdoor.WIN32.Kimsuky.A)

- Satellite broadcast giant DISH confirmed that 296,851 people were affected by the February ransomware attack, impacting their internal communications, call centers, and websites. Black Basta ransomware group is suspected to be behind this attack.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Win.BlackBasta; Ransomware_Linux_Basta)

- Researchers have reported on DarkCloud info-stealer, which is currently being distributed via spam emails. DarkCloud is designed to steal account credentials stored on infected systems. Recent campaigns have also observed the installation of ClipBanker malware alongside DarkCloud by threat actors.

  Check Point Threat Emulation provides protection against these threats (Trojan.Wins.Darkcloud.ta.A; Trojan.Win.Clipbanker.N; Trojan.Wins.Clipbanker.ta.*)

VULNERABILITIES AND PATCHES

- Barracuda Networks has disclosed that an RCE vulnerability (CVE-2023-2868) had impacted its Email Security Gateway (ESG) product. According to the company, the vulnerability allowed attackers unauthorized access to the gateways, until a patch was pushed by the company.
- D-Link, a Taiwanese networking solutions vendor, has fixed two critical vulnerabilities in its D-View 8 software. D-View 8 is a network management suite used for monitoring performance, device configurations, and more. The vulnerabilities (CVE-2023-32165 and CVE-2023-32169) could have allowed remote attackers to bypass authentication and execute arbitrary code.
- Zyxel has released a security advisory for several vulnerabilities (CVE-2023-33009 and CVE-2023-33010) capable of allowing unauthenticated RCE in their line of Firewall and VPN products. These buffer overflow vulnerabilities are also capable of inducing denial of service conditions.
- CISA has released four Industrial Control Systems (ICS) advisories on May 23, 2023. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

THREAT INTELLIGENCE REPORTS

- Check Point Research has disclosed a new ransomware family dubbed Moneybird that has been deployed by the Iranian APT group – Agrius. The group which was recently linked to Iranian Ministry of Intelligence and Security (MOIS) used this ransomware to target Israeli organizations.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.MoneyBird.*)

- Check Point Research has published a report on GuLoader - a prominent shellcode-based downloader that has been used in a large number of attacks to deliver a wide range of the “most wanted” malware. GuLoader’s payload is fully encrypted, what allows threat actors to store payloads using well-known public cloud services, and bypass antivirus protections.

  Check Point Threat Emulation provides protection against this threat (Dropper.Win.CloudEyE.*)

- Check Point Research elaborates on the latest Chinese state sponsored attacks and their use of network devices. This follows a joint Cybersecurity Advisory that United States and international cybersecurity authorities issued on Chinese state-sponsored cyber actor, also known as Volt Typhoon. This actor have compromised "critical" cyber infrastructure in a variety of industries, including governmental and communications organizations.
- Researchers have discovered a new ransomware family dubbed Obsidian ORB that targets Windows platforms. The group demands payment in the form of gift cards from popular online stores rather than traditional cryptocurrency ransom.